UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,767	10/22/2001	Mark Lucovsky	13768.198.6	4885

7590 01/25/2006

WORKMAN, NYDEGGER & SEELEY
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UT 84111

EXAMINER	
KIM, JUNG W	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 01/25/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/003,767	LUCOVSKY ET AL.	
	Examiner	Art Unit	
	Jung W. Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29 and 31-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29 and 31-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is in response to the amendment filed on December 9, 2005.

2. Claims 1-29 and 31-39 are pending.

3. Claims 1, 2, 10 and 31-36 are amended.

4. Claims 37-39 are new.

5. Claim 30 is canceled.

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Response to Amendment

7. The objections to claims 30 and 33 are withdrawn as the amendment overcomes the objections.

8. The 101 rejections to claims 30 and 33-35 are withdrawn as the amendment overcomes the 101 rejections.

Response to Arguments

9. Applicant's arguments, with respect to the prior art rejections have been fully considered and are persuasive. The 102 and 103 rejections as being unpatentable over primary reference Deinhart has been withdrawn. However, the subject matter of the instant claims are found to be unpatentable in view of the Wong disclosure "A Role-Based Access Control Model For XML Repositories" as outlined below. Further, in reply

to Applicant's argument that Wong does not defining a role definition by referencing a role template included in a role map document (Remarks, pg. 16, last paragraph), it is noted that the claims define role definitions as defining "access permissions for requesting entities by using one or more of the role templates." (claim 1) Based on this definition and related portions of the Specificaiton, as outlined below, it is identified that a "user" as taught by Wong covers the claimed limitation "role definition," since Wong discloses that a "user" is defined by a user_id, user_info and a rolepointer, which identifies a particular role. These characteristics correspond to the "role definition" as described in the claims.

Specification

10. The disclosure is objected to because of the following informalities: pg. 22, paragraph 56, first sentence: replace "XML documents will now listed and described" with –XML documents will now be listed and described--.

Claim Rejections - 35 USC § 102

> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

11. Claims 1-3, 5-9, 13-18, 24-29, 31-36, 38 and 39 are rejected under 35 U.S.C. 102(a) as being anticipated by Wong et al. "A Role-Based Access Control Model for XML Repositories" (hereinafter Wong).

12. As per claim 1, Wong discloses in a computer network that includes different types of data structures of one or more specific entities, a method for authorizing a requesting entity to operate upon data structures in a standard manner, the method comprising:

a. an act of maintaining a plurality of role templates that define basic access permissions with respect to one or more command methods, wherein at least some of the role templates define the basic access permissions in a manner that is independent of the type of data structure being operated upon (pg. 144, "role");

b. an act of maintaining a plurality of role definitions that define access permissions for requesting entities by using one or more of the role templates (pg. 144, "user", rolepointer points to a "role");

c. an act of receiving a request from the requesting entity to perform at least one of the command methods, the request identifying the requesting entity (pg. 142, expression (23), "normal request");

d. an act of identifying a role definition corresponding to the requesting entity (pg. 142, expressions (24) and (25)); and

e. an act of determining access permissions for the requesting entity with respect to the command method using the role definition corresponding to the requesting entity. (pg. 142, ACL performs step (d))

13. As per claim 2, Wong further discloses wherein the act of maintaining a plurality of role definitions that define access permissions for specific entities comprises:

f. an act of the role definition corresponding to the requesting entity using at least one access permission that is specific to the requesting entity, wherein the access permission for the requesting entity are defined by the one or more role templates that are used by the corresponding role definition as well as the access permission that is specific to the requesting entity. (pg. 142, login request, expression (22) and normal request, expression (23); pg. 144, "role" and "user")

14. As per claim 3, Wong further discloses wherein the request includes an identification of credentials used to authenticate the requesting entity, wherein the role definition corresponding to the requesting entity is identified using the credential identification, wherein different role definitions may apply depending on the credentials. (pg. 142, login request, expression (22); pg. 144, "user")

15. As per claim 5, Wong further discloses wherein the act of maintaining a plurality of role templates that define basic access permissions comprises the following: an act of maintaining a role map document that contains all of the role templates for a particular service. (pg. 144, <role_tree>)

16. As per claim 6, Wong further discloses wherein the act of maintaining a role map document that contains all of the role templates for a particular service comprises the following: an act of defining one or more scopes that describe views on a data structure;

and an act of defining a role template by associating a method type with one of the one or more scopes. (pg. 144, "acc_function" and "acc_operation"; each operation set is associated with a XML node)

17. As per claim 7, Wong further discloses wherein the act of maintaining a role map document that contains all of the role templates for a particular service comprises the following: an act of maintaining a role map document as a hierarchical data structure. (role_tree is a hierarchical data structure)

18. As per claim 8, Wong further discloses wherein the act of maintaining a role map document that contains all of the role templates for a particular service comprises the following: an act of maintaining a role map document as an XML document. (role_tree is an XML document)

19. As per claim 9, Wong further discloses wherein the act of maintaining a plurality of role definitions that define access permissions for specific entities by using one or more of the role templates comprises the following: an act of maintaining a role list document that contains all of the role definitions for requesting entities that may attempt to access data structures belonging to an identity. (pg. 144, < RBXAC_xml >)

20. As per claim 13, Wong further discloses wherein the act of receiving a request from the requesting entity to perform at least one of the command methods comprises

the following: an act of receiving a request from the requesting entity to insert a portion into the data structure. (pg. 142, normal request, "op"; pg. 144, "acc_operation")

21. As per claim 14, Wong further discloses wherein the act of receiving a request from the requesting entity to perform at least one of the command methods comprises the following: an act of receiving a request from the requesting entity to delete a portion from the data structure. (pg. 142, normal request, "op"; pg. 144, "acc_operation")

22. As per claim 15, Wong further discloses wherein the act of receiving a request from the requesting entity to perform at least one of the command methods comprises the following: an act of receiving a request from the requesting entity to update a portion of the data structure. (pg. 142, normal request, "op"; pg. 144, "acc_operation")

23. As per claim 16, Wong further discloses wherein the act of receiving a request from the requesting entity to perform at least one of the command methods comprises the following: an act of receiving a request from the requesting entity to replace a portion of the data structure. (pg. 142, normal request, "op"; pg. 144, "acc_operation")

24. As per claim 17, Wong further discloses wherein the act of receiving a request from the requesting entity to perform at least one of the command methods comprises the following: an act of receiving a request from the requesting entity to query regarding a portion of the data structure. (pg. 142, normal request, "op"; pg. 144, "acc_operation")

25. As per claim 18, Wong further discloses wherein the one or more command methods comprise a set including insert, delete, query, update, and replace. (pg. 142, normal request, "op"; pg. 144, "acc_operation")

26. As per claim 24, Wong further discloses wherein the data structure represents role list information. (pg. 141, section 7, the XML database stores both the ACL and the XML files; the access control file is stored in XML format)

27. As per claim 25, Wong further discloses wherein the data structure represents system information. (pg. 141, section 7, the XML database stores both the ACL and the XML files; the access control file is stored in XML format)

28. As per claim 26, Wong further discloses wherein the act of identifying a role definition corresponding to the requesting entity comprises: an act of identifying the role definition by searching a database. (pg. 142, expression (25))

29. As per claim 27, Wong further discloses wherein the act of identifying a role definition corresponding to the requesting entity comprises: an act of identifying the role definition based on authorized role information provided within the request. (pg. 142, login request, expression (22) and normal request, expression (23))

30. As per claim 28, Wong further discloses wherein the authorized role information includes an identification of a role template. (pg. 142 and 144, normal request includes a user_id, which identifies a user, which includes at least one rolepointer, which identifies at least one role)

31. As per claim 29, Wong further discloses wherein the authorized role information further includes an identification of at least one refined, local scope for modifying the role template. (pgs. 142 and 144, normal request includes a user_id, which identifies a user, which includes at least one rolepointer, which identifies at least one role, wherein each role includes an acc_function, which includes an XMLPointer; since each user id is associated with more than one role and/or each role has more than one XML node, each user id is associated with more than one scope).

32. As per claim 31, Wong discloses in a computer network that includes different types of data structures, a method for authorizing a requesting entity to operate upon data structures of one or more specific entities in a standard manner, the method comprising:

g. an act of maintaining a number of role templates that define basic access permissions with respect to a number of command methods, wherein at least some of the role templates define the basic access permissions in a manner that is independent of the type of data structure being operated upon (pg. 144, "role"); and

h. a step for authorizing a requesting entity using the role templates in a manner that is independent of the type of data structure being accessed. (pg. 142, normal request)

33. As per claim 32, Wong further discloses wherein the step for authorizing a requesting entity using the role templates comprises the following:

i. an act of maintaining a plurality of role definitions that define access permissions for receiving entities by using one or more of the role templates (pg. 144, "user");

j. an act of receiving a request from the requesting entity to perform at least one of the command methods, the request identifying the requesting entity (pg. 142, normal request);

k. an act of identifying a role definition corresponding to the requesting entity (pg. 142, expressions (24) and (25)); and

l. an act of determining access permissions for the requesting entity with respect to the command method using the role definition corresponding to the requesting entity (pg. 142, ACL performs step (d)).

34. As per claim 33, Wong further discloses wherein the act and step are performed by computer-executable instructions embodied within a physical computer-readable medium. (pgs. 141-142, section 7)

35. As per claim 34, Wong discloses computer program product for use in a computer network that includes different types of data structures of one or more specific entities, the computer program product for implementing a method for authorizing a requesting entity to operate upon data structures in a standard manner, the computer program product comprising one or more physical computer-readable media have stored thereon the following:

m. computer-executable instructions for maintaining a plurality of role templates that define basic access permissions with respect to one or more command methods, wherein at least some of the role templates define the basic access permissions in a manner that is independent of the type of data structure being operated upon (pg. 144, "role");

n. computer-executable instructions for maintaining a plurality of role definitions that define access permissions for receiving entities by using one or more of the role templates (pg. 144, "user", rolepointer points to a "role");

o. computer-executable instructions for detecting the receipt of a request from the requesting entity to perform at least one of the command methods, the request identifying the requesting entity (pg. 142, expression (23), "normal request");

p. computer-executable instructions for identifying a role definition corresponding to the requesting entity (pg. 142, expressions (24) and (25)); and

q. computer-executable instructions for determining access permissions for the requesting entity with respect to the command method using the role definition corresponding to the requesting entity (pg. 142, ACL performs step (d)).

36. As per claim 35, Wong further discloses wherein the one or more physical computer-readable media are storage media. (pgs. 141-142, section 7)

37. As per claim 36, Wong discloses in a computer network that includes different services, applications, and an authorization station, the applications submitting requests to perform operations on different data structures managed by the different services, a system for isolating the authorization process from the services so that the services need not independently authorize each request they receive from the number of applications, the system comprising:

r. a plurality of services, each service configured to facilitate operations on one or more types of data structures (pg. 138, section 1, "XML are usually stored in multiple sources or repositories");

s. an authorization station configured to receive requests from a number of applications to operate upon data structures managed by any of the number of services (pg. 142, 2nd essential component, ACL), the authorization station configured to perform the following:

i. receive a request from a requesting entity to perform a target operation upon a target data structure managed by a target service (pg.

142, login request and normal request, which identifies an operation and target);

ii. access a role template that defines basic authorizations with respect to one or more operations, including at least the target operation, wherein the role template defines the basic authorizations in a manner that is independent of the target data structure desired to be operated upon (pg. 142, expression (24) and (25); pg. 144, "role");

iii. determine that the corresponding requesting entity is authorized to perform the target operation on the target data structure (pg. 142, ACL performs step (d)); and

iv. communicate to the target service that the requesting entity is authorized to perform the target operation on the target data structure. (pg. 142, ACL performs step (d))

38. As per claim 38, Wong further discloses wherein the set of identifying a role definition corresponding to the requesting entity comprises the following:

t. an act of referencing a role template (pg. 144, "user"); and

u. an act of refining a scope referenced in the role template, wherein the refinement occurs at a user level. (144, "user", which includes at least one rolepointer, which identifies at least one role, wherein each role includes an acc_function, which includes an XMLPointer; since each user id is associated

with more than one role and/or each role has more than one XML node, each user id is associated with more than one scope)

39. As per claim 39, Wong further discloses wherein the act of determining access permissions for the requesting entity with respect to the command method using the role definition corresponding to the requesting comprises the following:

v. an act of determining access permissions below the data structure level. (pg. 144, "acc_function" includes an XMLPointer)

Claim Rejections - 35 USC § 103

40. Claims 4, 10-12 and 19-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wong.

41. As per claim 4, the rejection of claim 1 under 35 USC 102(a) as being anticipated by Wong is incorporated herein. (supra) Wong does not explicitly disclose the request identifies the requesting entity by identifying a user as well as a corresponding application that is making the request, wherein different role definitions may apply depending on both the identification of the user as well as the corresponding application. However, structured usernames (such as username@domain) are notoriously well-known identifications when making a request, wherein access is dependent on a structured username and a password. For example an ISP to authenticate a user on a RADIUS server submits a structured username. Examiner

takes Official Notice of this teaching. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the request to identify the requesting entity by identifying a user as well as a corresponding application that is making the request, wherein different role definitions may apply depending on both the identification of the user as well as the corresponding application. One would be motivated to do so since RADIUS authentication facilitates centralized authentication of users from a plurality of applications, which enables scalability. The aforementioned covers the limitations of claim 4.

42. As per claim 10, the rejection of claim 9 under 35 USC 102(a) as being anticipated by Wong is incorporated herein. (supra) In addition, Wong further discloses wherein the act of maintaining a role list document comprises the following: an act of defining a role definition by referencing a role template included in a role map document. (pg. 144, <RBXAC_xml>, <role_tree>) In the example, the elements are all defined in one configuration file such that the role map is not distinct from the role list, which is contrary to the limitation of claim 10, wherein the role map is distinct from the role list. However, this feature is an obvious enhancement to an XML document. It is notoriously well known to import entities into an XML document to enable a physical separation analogous to a logical separation. Examiner takes Official Notice of this teaching. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the role map and role list to be separate XML documents to facilitate better configuration design by establishing physical separation of distinct

entities as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 10.

43. As per claim 11, the rejection of claim 10 under 35 USC 103(a) as being unpatentable over Wong is incorporated herein. (supra) In addition, Wong further discloses wherein the act of maintaining a role list document comprises the following: an act of maintaining a role list document as a hierarchical data structure. (<RBXAC_xml > is a hierarchical data structure)

As per claim 12, the rejection of claim 10 under 35 USC 103(a) as being unpatentable over Wong is incorporated herein. (supra) In addition, Wong further discloses wherein the act of maintaining a role list document comprises the following: an act of maintaining a role list document as an XML document. (RBXAC_xml is an XML document)

44. As per claims 19-23, the rejection of claim 1 under 35 U.S.C. 102(a) as being anticipated by Wong is incorporated herein. (supra) Wong discloses the data structure represents general information in a computer system (pg. 1, Introduction; pg. 141, section 7), but Wong does not expressly disclose the data structure represents the following: in-box information, calendar information, document information, notification information or content information. However, it is notoriously well known for these types of information to be placed under access restriction: in-box information is specific to the receiver of the in-box; calendar information lists the personal obligations scheduled for a

given date; document information contains a litany of personal documents; notification information is private to the notifies; and content information relates to all of the above. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the data structure to represent any one of in-box information, calendar information, document information, notification information or content information, since all of these information require access restriction to maintain the privacy of the information as known to one of ordinary skill in the art. The aforementioned cover the limitations of claims 19-23.

45. Claim 37 is rejected under 35 USC 103(a) as being unpatentable over Wong in view of Stallings Cryptography and Network Security Chapter 11 (hereinafter Stallings).

46. As per claim 37, the rejection of claim 1 under 35 USC 102(a) as being anticipated by Wong is incorporated herein. (supra) Wong does not disclose the act of maintaining a plurality of role definitions that define access permissions for requesting entities by using one or more of the role templates comprises an act of maintaining a plurality of role definitions for the requesting entity, wherein the plurality of role definitions correspond to a plurality of authentication methods. Stallings discloses an authentication protocol, wherein a requesting user is authenticated by a central server to grant access into a particular server, wherein the particular server is one of a plurality of servers having their own authentication method (pgs. 329-335, "The Version 4 Authentication Dialogue"). In the user request to the central server, the user provides

his ID as well as the ID of a particular server to gain authentication to the particular server (pg. 331, Table 11.2, Message (1)). This type of authentication protocol consolidates a plurality of authentication methods into a access point, wherein a user has access rights to at least one of the plurality of servers. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the act of maintaining a plurality of role definitions that define access permissions for requesting entities by a using one or more of the role templates to comprise an act of maintaining a plurality of role definitions for the requesting entity, wherein the plurality of role definitions correspond to a plurality of authentication methods. One would be motivated to do so to gain the benefits of a centralized authentication service, such as scalability and security. (Stallings, pg. 325, 4 bullets) The aforementioned cover the limitations of claim 37.

Conclusion

47. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

48. Kuhn USPN 6,023,765 discloses an implementation of a role based access control in multi-level secure systems, wherein an RBAC system is implementing on a MLS system, thereby decoupling access permissions of a user from the targeted objects.

49. Vuong et al. 'Managing Security Policies in a Distributed Environment Using eXtensible Markup Language (XML)' discloses an example of implementing access controls using RBAC systems as XML.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

January 20, 2006

Jung W Kim
Examiner
Art Unit 2132

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100